

California Requires Privacy Policies to Address Consumer Tracking

September 2013

The California state legislature has passed, and Governor Jerry Brown is expected to sign, a bill (AB 370) that will require commercial websites to disclose how the operator responds to “Do Not Track” (DNT) indicators in Internet browsers, and whether other parties track consumers across their and other websites.

Privacy Policies

Since 2004, California law has required the operators of commercial websites that collect personally identifiable information (PII) from California residents to post privacy policies identifying the categories of information collected, with whom it may be shared, and how individuals may review that information. Because California is home to many leading Internet companies and has one of the largest economies on the planet, most commercial websites now publish such privacy policies. And the act of making privacy representations in a privacy policy will subject a website to the FTC's consumer protection jurisdiction, as well as that of the state attorney general.

The Amendment

The California legislature approved an amendment to the Business and Professions Code that would require a website operator to disclose “how the operator responds to web browser ‘Do Not Track’ signals” or similar technologies that allow consumers to express a choice regarding the collection of PII “about an individual consumer's online activities over time and across third-party websites or online services, if the operator engages in that collection.”

The amendment also would require disclosure of whether third parties, such as advertising networks, may collect PII about an individual's online activities over time and across different websites when using the operator's service.

This would be the first law at either the federal or the state level addressing DNT. DNT also remains the subject of contentious debate at the World Wide Web Consortium, as industry attempts to hash out a satisfactory standard for how websites should respond to DNT signals in browsers. And the FTC has encouraged industry to adopt DNT on a voluntary basis.

The legislation mandates *disclosure*; it does not *prohibit* tracking or behavioral targeting. However, websites that fail to disclose tracking or targeting could be deemed to have engaged in a misleading or deceptive trade practice. Therefore, website operators should review their sites' practices and consider the need to add language to their privacy policies to address DNT.